

RECEIVED  
CENTRAL FAX CENTER

SEP 12 2006

## REMARKS

In response to the rejection of claims 2, 14, and 16 under 35 U.S.C. §112, first paragraph, at page 2, paragraph 1 of the Office Action, Applicants have canceled claims 2 and 16 without prejudice or disclaimer. Additionally, with this response, claim 14 is amended to remove the term "JTRIP." Accordingly, Applicants request that the rejection of claims 2, 14, and 16 be withdrawn.

Applicants traverse the rejection of claims 1-27 under 35 U.S.C. §103(a) over U.S. Patent Publication No. 2004/0049693 ("Douglas") in view of U.S. Patent No. 6,081,894 ("Mann") at pages 2-5, paragraph 2 of the Non-Final Office Action. Douglas discloses a host-based intrusion detection sensor that monitors system logs, applications running on the host, and files for evidence of suspicious activity. *See Douglas, Abstract.* Douglas further discloses that, when suspicious activity is detected, the system notifies a system administrator. *See Douglas, Abstract.* Douglas further discloses that the device can take action to stop the suspicious event and record it for future forensic analysis. *See Douglas, p. 1, paragraph 0020.* The Office Action acknowledges that Douglas fails to disclose or suggest "in response to detection of the intrusion event, isolating the at least one network interface from the computer network and taking the host computer down to a single user state so that access to the host computer system is limited to physical access at the host computer system," as recited by independent claims 1 and 15.

The Office Action asserts that Mann discloses this feature, citing Mann at col. 3, lines 2-5. However, at the referenced section, Mann states:

When a virus is detected, a data isolator 60, that is responsive to a control signal 42 from the data comparator 40, isolates the first data channel 22 from the second data channel 32. Thus, viruses are detected and prevented from being received by the data receiving entity 30.

*See Mann, col. 3, lines 2-5.*

Thus, Mann fails to disclose isolating the at least one network interface from the computer network and taking the host computer system down to a single user state, as recited by independent claims 1 and 15. Mann discloses in Figure 1 that a data comparator 40 and a data

isolator 60 are between a data sending entity 20 and a data receiving entity 30, and that the data comparator 40 is to monitor traffic and to intercept malicious transmissions. *See Mann*, Figure 1 and col. 2 line 60 through col. 3, line 5. Mann further discloses that the isolating apparatus is a peripheral device that interfaces with a Peripheral Control Interface (PCI) bus of the receiving device to provide isolation from a data sending entity, such as the Internet. *See Mann*, col. 2, lines 8-12. The system of Mann detects a virus before it is received by the receiving entity and operates as an intrusion prevention system that isolates the receiving entity from the network to prevent the virus from being received at all. *See Mann*, col. 1, lines 38-41, lines 26-28 and col. 3, lines 2-5. Mann provides no indication that the peripheral device is adapted to take the receiving device down to a single user state, and, moreover, teaches away from a single user state, by stating:

A further advantage of the invention is that it isolates the data sending entity from the data receiving entity without disrupting normal operation of either entity.

*See Mann*, col. 2, lines 30-32.

By contrast, independent claims 1 and 15 recite “in response to detecting the intrusion event, isolating the at least one network interface from the computer network and taking the host computer system down to a single user state so that access to the host computer system is limited to physical access at the host computer system.” The “single user state” is different from normal operation in that “access to the host computer system is limited to physical access at the host computer system,” as recited by claims 1 and 15.

Accordingly, not only does Mann fail to disclose or suggest at least one claimed feature of claims 1 and 15, but Mann teaches away from the single user state, as recited by claims 1 and 15, by stating that the isolation is provided without disrupting normal operation. Mann therefore teaches away from the claimed invention of claims 1 and 15. Thus, even if the system of Douglas were combined with the isolation components of Mann, the resulting combination fails to disclose or suggest at least one element of independent claims 1 and 15, and of claims 3-13 and 17-27 at least by virtue of their dependency from one of claims 1 and 15.

Applicants traverse the rejection of claim 14 under 35 U.S.C. §103(a) over Douglas in view of Mann at page 5, paragraph 2 of the Office Action. Claim 14 recites in response to

detecting the intrusion event, the method includes issuing an IFCONFIG down command to the at least one network interface to isolate the at least one network interface from the computer network, issuing an INIT1 command to an operating system of the host computer system to take the host computer system down to a single user state, and writing a log of the intrusion event to a log database that is not located on the second computer system.

The Office Action rejects claim 14 over Douglas and Mann as applied to claims 1-8 and 10. As previously discussed, the asserted combination of Douglas and Mann fails to disclose or suggest at least one element of claims 1-10. Further, the asserted combination of Douglas and Mann fails to disclose or suggest in response to detecting the intrusion event, the method includes issuing an IFCONFIG down command to the at least one network interface to isolate the at least one network interface from the computer network, as recited by claim 14. Additionally, the asserted combination of Douglas and Mann fails to disclose or suggest issuing an INIT1 command to an operating system of the host computer system to take the host computer system down to a single user state, as recited by claim 14. Instead, Mann isolates a receiving entity from a sending entity, without disrupting normal operation of either entity. See *Mann*, col. 2, lines 29-31. As previously discussed and as acknowledged by the Office Action at page 3, paragraph 2, Douglas fails to disclose or suggest isolating the receiving device. Accordingly, the asserted combination of Douglas and Mann fails to disclose or suggest at least two elements of independent claim 14.

### CONCLUSION

Applicants have pointed out specific features of the claims not disclosed, suggested, or rendered obvious by the references applied in the Office Action. Accordingly, Applicants respectfully request reconsideration and withdrawal of each of the rejections, as well as an indication of the allowability of each of the pending claims 1, 3-15, and 17-27.

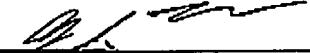
Any changes to the claims in this amendment, which have not been specifically noted to overcome a rejection based upon the prior art, should be considered to have been made for a purpose unrelated to patentability, and no estoppel should be deemed to attach thereto.

The Examiner is invited to contact the undersigned attorney at the telephone number listed below if such a call would in any way facilitate allowance of this application.

The Commissioner is hereby authorized to charge any fees, which may be required, or credit any overpayment, to Deposit Account Number 50-2469.

Respectfully submitted,

9-11-2006  
\_\_\_\_\_  
Date

  
\_\_\_\_\_  
Jeffrey G. Toler, Reg. No. 38,342  
Attorney for Applicant(s)  
TOLER SCHAFFER, L.L.P.  
5000 Plaza On The Lake, Suite 265  
Austin, Texas 78746  
(512) 327-5515 (phone)  
(512) 327-5575 (fax)

JGT/RMR